(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11143833 A**

(43) Date of publication of application: **28 . 05 . 99**

(51) Int. Cl **G06F 15/00**
G09C 1/00
H04L 9/32

(21) Application number: **09313390**

(22) Date of filing: **14 . 11 . 97**

(71) Applicant: **TOSHIBA CORP**

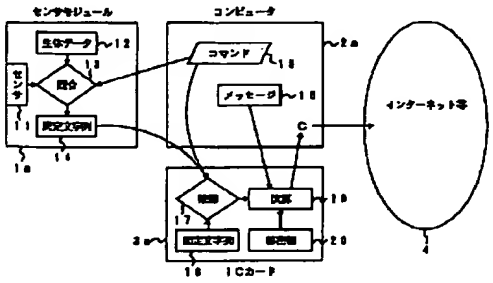
(72) Inventor: **YAMADA KOUKI**

(54) USER CONFIRMATION SYSTEM AND IC CARD BY BIOLOGICAL DATA AND STORAGE MEDIUM

(57) Abstract:

PROBLEM TO BE SOLVED: To make it possible to protect biological data with high safety by putting them in a management range at hand of a user and to reduce a feeling of resistance and a risk of leakage of the biological data.

SOLUTION: This user confirmation system consists of a sensor 11 for performing a biological measurement, a biological data holding part 12 for holding biological data, a tamper proof sensor module 1a that is equipped with a collating calculation part 13 which collates measurement information measured by the sensor with the biological data in the biological data holding part and outputs a notification of the fact when a person concerned is confirmed by the collated result, an IC card 3a that performs a data output by corresponding to that a user confirmation is made when the notification is received, a confirmation processing part 17, an operation processing part 19 and a communication means 2a for performing a communication between the sensor module and the IC card.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－143833

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ

審査請求　未請求　請求項の数15　ＯＬ　（全 22 頁）

(21)出願番号　特願平9－313390

(22)出願日　平成９年(1997)11月14日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　山田　貢己
東京都府中市東芝町１番地　株式会社東芝府中工場内

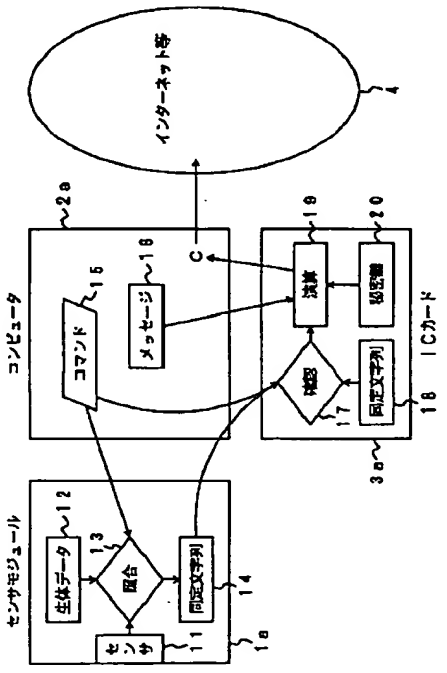
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　生体データによるユーザ確認システム及びＩＣカード並びに記録媒体

(57)【要約】

【課題】　生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ユーザの抵抗感及び生体データの漏洩危険性を低減する。

【解決手段】　生体測定を行うセンサ１１、生体データを保持する生体データ保持部１２、並びに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部１３を備えた耐タンパー性のセンサモジュール１ａと、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するＩＣカード３ａ，１７，１９と、センサモジュールとＩＣカードとの間の通信を行う通信手段２ａとからなる生体データによるユーザ確認システム。



1

【特許請求の範囲】

【請求項１】　生体測定を行うセンサ、生体データを保持する生体データ保持部、並びに、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えた耐タンパー性のセンサモジュールと、

前記通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するＩＣカードと、

前記センサモジュールと前記ＩＣカードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項２】　生体測定を行うセンサを備えたセンサモジュールと、

生体データを保持する生体データ保持部、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部、並びに、前記通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、

前記センサモジュールと前記ＩＣカードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項３】　生体測定を行うセンサ、暗号化された生体データを受信しこれを復号化する復号部、並びに、前記センサにより測定された測定情報と復号化された前記生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたセンサモジュールと、

前記暗号化された生体データを保持するとともに、当該暗号化された生体データを前記センサモジュールに送出する生体データ保持部、並びに、前記照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、

前記センサモジュールと前記ＩＣカードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項４】　前記センサモジュールに耐タンパー性を持たせたことを特徴とする請求項３記載の生体データによるユーザ確認システム。

【請求項５】　生体測定を行うセンサを備えたセンサモジュールと、

暗号化された生体データを受信しこれを復号化する復号部、並びに、前記センサにより測定された測定情報と復号化された前記生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたコンピュータと、

前記暗号化された生体データを保持するとともに、当該暗号化された生体データを前記コンピュータに送出する生体データ保持部、並びに、前記照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、

前記センサモジュールと前記ＩＣカードと前記コンピュータとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項６】　前記ＩＣカードはユーザ本人のデジタル署名を行う署名手段を備え、前記ユーザ確認がされたことに対応してなされるデータ出力には、前記署名手段によるデジタル署名が含まれることを特徴とする請求項１乃至５のうち何れか１項記載の生体データによるユーザ確認システム。

【請求項７】　生体測定を行うセンサを備えたセンサモジュールと、

ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持部、並びに、前記ユーザ要求及び前記ログオンパスワードが入力されたときに前記生体データ保持部の生体データを前記ログオンパスワードにより復号化するとともに、この復号化された生体データと前記センサにより測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、前記ユーザ要求を実施すべき旨の通知を出力する照合計算部を備えたコンピュータと、

前記コンピュータと前記センサモジュールとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項８】　生体測定を行うセンサと、コンピュータと、ＩＣカードとからなり、ユーザ確認を行うとともにデータの暗号化処理を行うユーザ確認システムにおいて、

前記ＩＣカードは、耐タンパー性を有し、かつ、生体データを保持する生体データ保持部、前記データの暗号化処理におけるその一部処理を実行する第１の暗号計算部、並びに、前記第１の暗号計算部での処理に用いられる暗号鍵を保持する暗号鍵保持部を少なくとも備えており、

前記コンピュータは、ユーザ確認通知を受けると前記データの暗号化処理における他の処理を実行する第２の暗号計算部を少なくとも備えており、

さらに、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときには前記第２の暗号計算部に前記ユーザ確認通知を出力する照合計算手段と、

前記センサと前記ＩＣカードと前記コンピュータとの間の通信を行う通信手段とからなることを特徴とする生体

2

データによるユーザ確認システム。

【請求項９】　コンピュータに、

ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持機能と、

前記ユーザ要求及び前記ログオンパスワードが入力されたときに前記生体データを前記ログオンパスワードにより復号化するとともに、この復号化された生体データと生体測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、前記ユーザ要求を実施すべき旨の通知を出力する照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　コンピュータに、

ユーザ確認通知を受けた場合には、データの暗号化処理における一部処理を実行するとともに、このデータ暗号化処理における他の処理の処理結果を外部から受け取り、その処理結果を前記一部処理が用いて暗号化処理を完成させる暗号計算機能と、

生体測定された測定情報とユーザ確認用の生体データとを照合するとともに、照合結果よりユーザ本人と確認されたときには前記暗号計算機能に前記ユーザ確認通知を行う照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１１】　暗号化された生体データを保持するとともに、この暗号化された生体データを外部装置に出力する生体データ保持手段と、

前記生体データと生体測定された測定情報とによりユーザ本人と確認された旨の照合結果を前記外部装置から通知されると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理手段とを備え、かつ耐タンパー性を有することを特徴とするＩＣカード。

【請求項１２】　前記外部装置は、生体測定を行うセンサを有するセンサモジュールであることを特徴とする請求項１１記載のＩＣカード。

【請求項１３】　前記外部装置は、コンピュータであることを特徴とする請求項１１記載のＩＣカード。

【請求項１４】　前記演算処理手段はユーザ本人のデジタル署名を行う署名手段を備え、前記ユーザ確認がされたことに対応してなされるデータ出力には、前記署名手段によるデジタル署名が含まれることを特徴とする請求項１１乃至１３のうち何れか１項記載のＩＣカード。

【請求項１５】　生体データを保持するとともに、この生体データを用いてユーザ確認を行う外部装置に前記生体データを出力する生体データ保持手段と、

データの暗号化処理における一部処理を暗号鍵を用いて実行するとともに、このデータの暗号化処理における他の処理を行う外部装置に前記一部処理の処理結果を出力する暗号計算手段と、

前記暗号鍵を保持する暗号鍵保持手段とを備え、かつ耐タンパー性を有することを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＩＣカードを利用したデジタル署名処理や、計算機ソフトウェアの使用権限確認、あるいはデータ暗号化処理の使用権限確認等を便利且つ安全に行うための生体データによるユーザ確認システム及びＩＣカード並びに記録媒体に関する。

【０００２】

【従来の技術】従来からユーザを確認するのにクレジットカードや入退室管理カード等，主に磁気カードが使われている。これに対し、最近、カードの偽造や情報漏洩を防ぐ効果等を期待して、半導体チップを内蔵した高セキュリティで高機能のＩＣカードが使われ始めている。

【０００３】しかしながら、ＩＣカードを利用しても、紛失や盗難により他人に不正使用されたり、紛失と偽って不正使用することに対して、それを防ぐことが難しい。

【０００４】ＩＣカードに対応したパスワードを登録することにより不正使用を減らそうとすることが行われているが、パスワードは記憶することが煩わしく、忘れてしまう危険性や、メモを他人に読まれたりして漏洩する危険性があり、決して便利であるとは言えない。

【０００５】最近では、指紋や掌型のような生体データを測定して本人を確認する技術であるバイオメトリクスとＩＣカードとを組み合わせて入退室管理やアクセス制御を行おうとする動きがある。これによって、カードの紛失、盗難、漏洩、忘却等により生じる各種問題は解決すると思われる。

【０００６】しかし、一方でパスワードのような自由に創造できるものではなく唯一無二の自分の身体の情報（生体データ）がどこかに登録されているということに対するユーザの抵抗感や、それが漏洩したときにパスワードのような変更が効かないという弱点及び漏洩トラブルに対するユーザの不安感が根強く残っている。したがって、バイオメトリクスをユーザ確認に用いる場合には、上記抵抗感が少なくなるような技術を提案し、また、生体データの漏洩を効果的に防止できるシステムを構築する必要がある。

【０００７】さらに、通常ＩＣカードを用いないことの多い計算機ソフトウェアの使用権限確認を行う環境においては、生体データを安全に保持する媒体が無く、バイオメトリクスを利用する場合には生体データを計算機の記憶媒体上に格納するしかない。しかし、この場合にはリバースエンジニアリングによって生体データが漏洩する危険性がある。

【０００８】

【発明が解決しようとする課題】上述したように、従来のＩＣカードとパスワードを併用する技術では、煩わし

さ、忘却あるいは漏洩の危険性といった問題点がある。

【０００９】また、ＩＣカードとバイオメトリクスの併用では、自分の身体の情報（生体データ）が登録されることへの抵抗感や、生体データが第三者へ漏洩する危険性が残っている。

【００１０】さらに、ＩＣカードを用いない環境においてバイオメトリクスを利用して使用権限の確認をする場合には、生体データを安全に記録する方法が無かった。

【００１１】本発明は、上記事情を考慮してなされたもので、生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感及び生体データの漏洩危険性を低減することを可能とし、さらに使用上の煩わしさが少なくユーザ確認の確実性が高い生体データによるユーザ確認システム及びＩＣカード並びに記録媒体を提供することを目的とする。

【００１２】

【課題を解決するための手段】上記課題を解決するために、請求項１に対応する発明は、生体測定を行うセンサ、生体データを保持する生体データ保持部、並びに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えた耐タンパー性のセンサモジュールと、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するＩＣカードと、センサモジュールとＩＣカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【００１３】本発明はこのような手段を設けたので、生体データ保持部内の生体データが耐タンパー性のセンサモジュールに保護され、生体データを高い安全性でもって守ることができ、生体データの漏洩危険性を低減するとともに、さらに使用上の煩わしさを少なくしユーザ本人確認の確実性を高くすることができる。

【００１４】次に、請求項２に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、生体データを保持する生体データ保持部、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部、並びに、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、センサモジュールとＩＣカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【００１５】本発明はこのような手段を設けたので、請求項１に対応する発明と同様な効果が得られる他、生体データ保持部を耐タンパー性のＩＣカードに設けたことで生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感を低減させることができる。

【００１６】次に、請求項３に対応する発明は、生体測定を行うセンサ、暗号化された生体データを受信しこれを復号化する復号部、並びに、センサにより測定された測定情報と復号化された生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたセンサモジュールと、暗号化された生体データを保持するとともに、当該暗号化された生体データを前記センサモジュールに送出する生体データ保持部、並びに、照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、センサモジュールとＩＣカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【００１７】本発明はこのような手段を設けたので、請求項２に対応する発明と同様な効果を得ることができる。

【００１８】また、請求項４に対応する発明は、請求項３に対応する発明において、センサモジュールに耐タンパー性を持たせた生体データによるユーザ確認システムである。

【００１９】本発明はこのような手段を設けたので、請求項３に対応する発明と同様な効果を得ることができる他、生体データ等の安全性を一層高めることができる。

【００２０】さらに、請求項５に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、暗号化された生体データを受信しこれを復号化する復号部、並びに、センサにより測定された測定情報と復号化された生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたコンピュータと、暗号化された生体データを保持するとともに、当該暗号化された生体データをコンピュータに送出する生体データ保持部、並びに、照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のＩＣカードと、センサモジュールとＩＣカードとコンピュータとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【００２１】本発明はこのような手段を設けたので、請求項２に対応する発明と同様な効果をある程度は得られるとともに、簡易にかつ安価なシステムを構築することができる。

【００２２】さらにまた、請求項６に対応する発明は、請求項１～５に対応する発明において、ＩＣカードはユーザ本人のデジタル署名を行う署名手段を備え、ユーザ確認がされたことに対応してなされるデータ出力には、署名手段によるデジタル署名が含まれる生体データによるユーザ確認システムである。

【００２３】本発明はこのような手段を設けたので、請求項１～５に対応する発明と同様な効果が得られる他、

ＩＣカードを用いたデジタル署名システムを構築することができる。

【００２４】一方、請求項７に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持部、並びに、ユーザ要求及びログオンパスワードが入力されたときに生体データ保持部の生体データをログオンパスワードにより復号化するとともに、この復号化された生体データとセンサにより測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、ユーザ要求を実施すべき旨の通知を出力する照合計算部を備えたコンピュータと、コンピュータとセンサモジュールとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【００２５】本発明はこのような手段を設けたので、パスワードで暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。また、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、使用上の煩わしさを少なくしユーザ本人確認の確実性を高くすることができる。

【００２６】また、請求項８に対応する発明は、生体測定を行うセンサと、コンピュータと、ＩＣカードとからなり、ユーザ確認を行うとともにデータの暗号化処理を行うユーザ確認システムにおいて、ＩＣカードは、耐タンパー性を有し、かつ、生体データを保持する生体データ保持部、データの暗号化処理におけるその一部処理を実行する第１の暗号計算部、並びに、第１の暗号計算部での処理に用いられる暗号鍵を保持する暗号鍵保持部を少なくとも備えており、コンピュータは、ユーザ確認通知を受けるとデータの暗号化処理における他の処理を実行する第２の暗号計算部を少なくとも備えており、さらに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときには第２の暗号計算部にユーザ確認通知を出力する照合計算手段と、センサとＩＣカードとコンピュータとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【００２７】本発明はこのような手段を設けたので、生体データ及び暗号鍵が耐タンパー性の高いＩＣカードに格納され、確実なユーザ本人確認がなされた後に暗号化処理を実行することができる。また、ＩＣカードとコンピュータとで暗号化処理を分担するようにしているので、極めて秘匿性の高い暗号化を実現することができる。

【００２８】さらに、請求項９に対応する発明は、コンピュータに、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持機能と、ユーザ要求及びログオンパスワードが入力されたときに生体データをログオンパスワードにより復号化するとともに、この復号化された生体データと生体測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、ユーザ要求を実施すべき旨の通知を出力する照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００２９】本発明はこのような手段を設けたので、請求項７に記載した生体データによるユーザ確認システムにおけるコンピュータの動作を実現させることができる。

【００３０】さらにまた、請求項１０に対応する発明は、コンピュータに、ユーザ確認通知を受けた場合には、データの暗号化処理における一部処理を実行するとともに、このデータ暗号化処理における他の処理の処理結果を外部から受け取り、その処理結果を用いて暗号化処理を完成させる暗号計算機能と、生体測定された測定情報とユーザ確認用の生体データとを照合するとともに、照合結果よりユーザ本人と確認されたときには暗号計算機能にユーザ確認通知を行う照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００３１】本発明はこのような手段を設けたので、請求項８に記載した生体データによるユーザ確認システムにおけるコンピュータの動作を実現させることができる。

【００３２】一方、請求項１１に対応する発明は、暗号化された生体データを保持するとともに、この暗号化された生体データを外部装置に出力する生体データ保持手段と、生体データと生体測定された測定情報とによりユーザ本人と確認された旨の照合結果を外部装置から通知されると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理手段とを備え、かつ耐タンパー性を有することを特徴とするＩＣカードである。

【００３３】本発明はこのような手段を設けたので、請求項３又は５に記載した生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００３４】次に、請求項１２に対応する発明は、請求項１１に対応する発明において、外部装置は、生体測定を行うセンサを有するセンサモジュールであるＩＣカードである。

【００３５】本発明はこのような手段を設けたので、請求項３又は４に記載した生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００３６】また、請求項１３に対応する発明は、請求項１１に対応する発明において、外部装置は、コンピュ

ータであるＩＣカードである。

【００３７】本発明はこのような手段を設けたので、請求項５に記載した生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００３８】さらに、請求項１４に対応する発明は、請求項１１～１３に対応する発明において、演算処理手段はユーザ本人のデジタル署名を行う署名手段を備え、ユーザ確認がされたことに対応してなされるデータ出力には、署名手段によるデジタル署名が含まれるＩＣカードである。

【００３９】本発明はこのような手段を設けたので、請求項３～５に対応する発明のうち、さらに請求項６の手段も有する生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００４０】また、請求項１５に対応する発明は、生体データを保持するとともに、この生体データを用いてユーザ確認を行う外部装置に生体データを出力する生体データ保持手段と、データの暗号化処理における一部処理を暗号鍵を用いて実行するとともに、このデータの暗号化処理における他の処理を行う外部装置に一部処理の処理結果を出力する暗号計算手段と、暗号鍵を保持する暗号鍵保持手段とを備え、かつ耐タンパー性を有するＩＣカードである。

【００４１】本発明はこのような手段を設けたので、請求項８に記載した生体データによるユーザ確認システムにおけるＩＣカードの動作を実現させることができる。

【００４２】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

【００４３】本発明は、すでに述べたように、１）生体データの漏洩危険性を低減させること、２）自己の生体データを情報機器を格納することに対するユーザの抵抗感を低減させること、を目的としており、上記１）、２）の何れか若しくは両方を実現できる手段を提供するものである。

【００４４】特に、発明者らは、生体データによるユーザ確認システムの一形態としてのＩＣカード署名システムに、バイオメトリクスを適用させる場合にいかなるシステムを構築すれば上記目的を実現できるかについて種々検討した。ここで、ＩＣカード署名システムとは、ＩＣカード内部のデジタル署名機能を作動させる機能をもったＩＣカードを利用し、そのデジタル署名により、機密情報の電子メールによる送付、インターネット上の買い物等を実現させるシステムである。このシステムにバイオメトリクスを適用させた場合には、指紋等の生体データについてのセンサ測定情報との照合結果に基づき本人確認を行い、その上でＩＣカードの上記デジタル署名機能を作動させることになる。

【００４５】発明者らは、まず、バイオメトリクスを適用させたＩＣカード署名システム（以下、単にＩＣカード署名システム又はシステムともいう）を構成し得る要素として４つのモジュール、つまりＩＣカード、センサモジュール、コンピュータ（ＰＣ、ＩＣカードリーダ／ライタ含む）、サーバーについて検討した。次に、ＩＣカード署名システムにおいて行われる処理（生体（登録）データ記録、照合計算）をそれぞれどのモジュールで行えば本発明の目的を達成できるかについて検討した。

【００４６】図１５はバイオメトリクスを適用させたＩＣカード署名システムにおける構成要素及びその組み合わせ結果を示す図である。

【００４７】図１５に示す各候補システムのうち、生体データがユーザの手元には無い中央処理装置に登録されることを嫌うユーザが存在することを考慮し、ローカルな処理によってＩＣカードの所有者確認を行うことを優先する。そのためサーバーを利用するものは、検討のこの時点では除外した。生体データをユーザ手元の管理範囲に置いて守ることができるシステムであれば、ユーザの抵抗感を低減させることができると考えられるからである。ただし、技術成果の結実である発明を解釈するに当たり、上記ユーザ抵抗感に関し特に問題がない場合には、請求項に記載された範囲内であれば、サーバー等を利用する技術も発明範囲に含まれるものである。

【００４８】次に、同一の端末（センサ、ＰＣ）を不特定多数で使用可能であること、さらに、同一人物が不特定の端末で使用可能であることの利便性を考慮し、ＩＣカードに生体データを保持するものは候補システムとして残した。

【００４９】なお、生体データ保持と照合計算部を一つの耐タンパー性のモジュール内（ＩＣカード又はセンサモジュール）においたものは候補とした残した。この場合、生体データ～照合計算部間の通信が不要となりプロトコルが単純になり、セキュリティも高くできるからである。ここで、耐タンパー性とは、内部の物や情報を原形のまま容易には外部に取り出せないような仕組みを有した性質のことである。この耐タンパー性を実現するには種々の方法が考えられるが、その方法の具体的な例については後述する。

【００５０】こうして図１５に示すように、多くの組み合わせの中から特に有効と思われる候補システムを５つ見出した。なお、同図中、「ＰＩＮ」と記したものは、ＩＣカードとＰＣ等との間で機器認証を行うための識別コードであり、署名鍵とは区別している。

【００５１】以下、図１５に示す候補システムに対応してなされた発明について第１の実施形態から第５の実施形態において説明し、さらに、同図に示さない他のシステムについて第６の実施形態から第８の実施形態において説明する。

【００５２】（発明の第１の実施の形態）図１は本発明の第１の実施の形態に係る生体データによるユーザ確認

システムの一例を示す構成図である。

【００５３】このユーザ確認システムは、図１５の候補システムのうちの耐タンパーモジュール一体型であり、センサモジュール１ａと、コンピュータ２ａと、ＩＣカード３ａとから構成されている。このシステムでは、センサモジュール１ａ側で生体データ保持と照合計算を行い、ＩＣカード３ａ側では署名処理のみを行うセンサモジュール１ａは、センサ１１と、生体データ保持部１２と、照合処理部１３と、同定文字列格納部１４とから構成されている。なお、特に図示しないが、このセンサモジュール１ａには、ＣＰＵ、メモリ等が内蔵され、各種情報処理が実行できるようなっている。

【００５４】ここで、センサ１１は、生体測定として指紋を測定し電子化情報とする手段であり、生体データ保持部１２には各ユーザの生体データが格納されている。また、照合計算部１３は、測定されたセンサ情報と生体データを照合し、ユーザ本人か否かを判定するとともに、ユーザ本人であった場合には、その旨の出力を通知する手段である。なお、本実施形態では、照合処理部１３は、同定文字列格納部１４の同定文字列（以下単にパスワードともいう）をコンピュータ２ａを介してＩＣカード３ａに出力するようになっている。

【００５５】ここで、センサモジュール１ａは、スタンドアロン型であり、耐タンパー性を有するものである。なおスタンドアロン型とは耐タンパーセンサモジュール内に少なくともセンサ１１と照合計算部１３を持つものである。このシステムのセキュリティは、主にセンサモジュール１ａ内の生体データと照合計算部１３の耐タンパー性によっている。このために、センサモジュール１ａにおけるセンサ１１以外の各部が１チップのＩＣにより構成されている。また、モジュール各構成部分は強固な筐体に格納され、その蓋が開かないようになっている。さらに、強制的に蓋を開けると、生体データ保持部１２、照合処理部１３及び同定文字列格納部１４が格納されるＩＣチップ自体が破壊されるような仕組みになっている。本実施形態ではこの筐体を壁に埋め込んで更なる耐タンパー性を確保している。

【００５６】また、センサ１１以外の各部１２，１３，１４を１チップのＩＣで構成したこと自体が耐タンパー性を確保することにつながっている。例えばパスワード情報を磁気カードに格納した場合、磁気カードにはその磁気テープ表面に情報がそのまま保持されているので、情報保持の構造さえわかれば容易に上記パスワード情報を読み取ることができ、耐タンパー性が低い。これに対してＩＣチップに情報を格納する場合は、そのチップ端子からコマンド等を電気信号として入力して初めて情報が端子から得られることになる。この操作を実行するのは高い技術が必要であり、その分耐タンパー性が高いと言える。

【００５７】また、本実施形態の場合、生体データは同一のＩＣチップ内でのみ使用されるため、外部出力は不要であり、耐タンパー性を高めるべく生体データの外部出力はできないように構成されている。

【００５８】なお、本明細書において、耐タンパー性を有するといった場合には、上記仕組みの何れかあるいはすべてが組み合わされ、また、その他の考え得る措置が取られているものである。また、ここでは、センサモジュールの場合で説明したが、ＩＣカード等の場合でも同様な措置により耐タンパー性を高めることができる。特に、ＩＣカードの場合は、例えばその筐体を開くと鉄粉が配線上に飛び散り、保持情報をすべて消失させるような仕組みを設けることも可能である。

【００５９】また、最低限の議論として、単に耐タンパー性があるかないかを考えるときには、例えば保護したい内容が１つのＩＣチップ内に納められているような場合には耐タンパー性はあると言えるであろう。

【００６０】次に、コンピュータ２ａには、コマンド出力部１５と、メッセージ出力部１６とが設けられている。また、コンピュータ２ａにはＩＣカードリーダ&ライタが含まれ、この点は以下の各実施形態でも同様である。

【００６１】さらにコンピュータ２ａは特に図示しないが、ブラウザ等の種々のアプリケーションプログラムを実行することが可能であり、本実施形態ではインターネット４に接続されている。

【００６２】インターネット４では更にバーチャルモールに接続されており、コンピュータ２ａからオンラインショッピングができるようになっている。コンピュータ２ａに示される符号「Ｃ」は演算（デジタル署名処理等）されたメッセージであるが、後述する本実施形態の動作例ではバーチャルモールに対する物品購入等の要求出力を示している。

【００６３】ＩＣカード３ａは、確認処理部１７と、同定文字列格納部１８と、演算処理部１９と、秘密鍵保持部２０とを備えており、これら各部を実現するＣＰＵやメモリ等の資源が１チップのＩＣに納められたものである。

【００６４】確認処理部１７は、センサモジュール１ａからの同定文字列をＩＣカード内の同定文字列格納部１８に格納された同定文字列（パスワード）と比較し、その確認結果を演算処理部１９に通知する。つまり、センサモジュール１ａとＩＣカード３ａは、本人が確認されたか否かの情報をセンサモジュールからＩＣカードへ秘密裏に伝えるための同定文字列を共有していることになる。具体的には、ＩＣカード側の同定文字列はセンサモジュール側の同定文字列と同一であるか、或いは、ちょうどＵＮＩＸにおける暗号化パスワードのように、センサモジュール側の同定文字列を暗号化したものでもよい。要するにセンサモジュールから送られた同定文字列に対応して唯一のＩＣカード内同定文字列が対応するよ

うになっている。

【００６５】演算処理部１９は、システム使用者がユーザ本人であることの確認通知を確認処理部１７から受けると、所定の演算処理を実行して、演算されたメッセージＣを出力する。このメッセージは、例えば入室管理上の扉開メッセージでもよいし、また例えば計算機等の装置起動命令でもよい。ここで演算処理部１９は具体的な一例として、秘密鍵保持部２０に格納される秘密鍵を用いてデジタル署名を行うとともに、メッセージ出力部１６の情報を元にインターネット上のバーチャルモールに物品購入要求を演算されたメッセージＣとして出力する。

【００６６】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【００６７】上記したように生体データによるユーザ確認システムは種々の場合に適用できるが、ここでは、インターネット上のバーチャルモールに物品購入要求を出力する場合を例にとってその動作例を説明する。

【００６８】図２は本実施形態の動作例を示す流れ図である。

【００６９】この動作例では、自宅や会社でコンピュータ２ａとしてのパーソナルコンピュータ（パソコン）を立ち上げブラウザソフトを起動し、インターネット４さらにはバーチャルモールに接続して物品購入をしようとする場合を想定している。

【００７０】ユーザは、バーチャルモールにおいて商品及びその購入数量を選択決定し、パソコン上の購入ボタンをクリックする。この操作により図１に示すようにコンピュータ２ａからコマンド１５がセンサモジュール１ａ及びＩＣカード３ａに出力され、各種指示等の表示がコンピュータ２ａ上になされる（ＳＴ１）。

【００７１】ここで、ＩＣカード３ａがシステムに未挿入の場合には、コンピュータ２ａから「ＩＣカードを挿入してください」とのメッセージが出され、ユーザによりＩＣカード３ａが挿入される（ＳＴ２）。なお、カード挿入に伴いコンピュータ２ａから当該カード３ａに物品購入処理が開始されたことが通知（コマンド１５）される。

【００７２】次に、ユーザが自分の指をセンサモジュール１ａのセンサ１１に押し当てると、センサ１１による生体測定が実行される（ＳＴ３）。

【００７３】次に、測定されたセンサ情報はセンサモジュール１ａの照合計算部１３において生体データと照合され（ＳＴ４）、本人が確認されれば（ＳＴ５）、同定文字列格納部１４内の同定文字列（パスワード）がＩＣカード３ａに出力される（ＳＴ６）。なお、この処理は、従来システムにおけるパスワードのキー入力に代わるものである。また、センサモジュール１ａからＩＣカード３ａへの同定文字列送出において、ハッカーによる同定文字列の盗聴の危険性を排除するためには、同定文字列を生で送る代わりに暗号化すればよい。

【００７４】また、ステップＳＴ５において、本人が確認できない場合には、システム使用者がユーザ本人でない旨が表示され、以降の処理は中止される。

【００７５】ＩＣカード３ａの確認処理部１７においては、受信した同定文字列がカード内の保持された同定文字列と比較され、システム使用者がユーザ本人であることが確認される（ＳＴ７）。本人確認がなされればその旨が演算処理部１９に通知される。

【００７６】本人確認の通知を受けた演算処理部１９により、メッセージ出力部１６からの物品購入情報に基づいてメッセージＣが作成されるとともに、そのメッセージＣには秘密鍵保持部２０に保持される秘密鍵によりデジタル署名が行われる（ＳＴ８）。

【００７７】こうして作成され演算されたメッセージＣは、コンピュータ２ａからインターネット４に出力され、バーチャルモールでの物品購入が実現されることになる。

【００７８】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、生体データ保持部１２と生体データによる照合を行う照合計算部１３とを同一のセンサモジュール１ａ内に格納して生体データがセンサモジュール１ａ外に出力しないようにし、かつ、センサモジュール１ａ自体に高い耐タンパー性を持たせたので、生体データの漏洩危険性をほとんど無くすことができ、ひいてはこれによって自己の生体データを情報機器を格納することに対するユーザの抵抗感を低減させることができる。

【００７９】また、デジタル署名等を行うに際してパスワード入力でなく、本人への生体測定に基づきユーザ確認をするようにしているので、極めて確実性の高い本人確認を行うことができる。したがって、例えばＩＣカードが紛失したり、盗まれた場合でも第３者による悪用を防止することができる。

【００８０】さらに、本システムでは、照合計算部１３による照合ののち、その結果をパスワードを用いて演算処理部１９に通知するようにしたので、本人を確認してからデジタル署名するまでの処理を安全に行うことができ、極めてセキュリティの高いＩＣカード署名システムを実現することができる。したがって、例えばＩＣカードを含めたシステム全体が盗まれるようなことがあっても、盗難者は生体データを得ることも偽のメッセージＣを出力することもできない。なお、このような場合に、秘密鍵や同定文字列が漏洩しないようにＩＣカード３ａ自体にも高い耐タンパー性が与えられている。

【００８１】また、本実施形態のシステムではバイオメトリクスを利用しているので、パスワード等を記憶しておく必要もなく、パスワード入力の煩わしさやその忘却、漏洩の危険性のないシステムを提供することができ

る。

【００８２】さらに、本実施形態では、センサ１１、生体データ保持部１２、照合処理部１３、同定文字列格納部１４、確認処理部１７、同定文字列格納部１８、演算処理部１９及び秘密鍵保持部２０の各構成要件を図１に示すようにセンサモジュール１ａ及びＩＣカード３ａに配置したので、上記各効果の他、ＩＣカード利用上のメリットも得られる。つまり、従来の署名用のＩＣカードをほとんどそのまま利用することができる。その意味で、本実施形態は既カード利用型とも言える。指紋照合処理の採用を念頭に入れた特殊なＩＣカードを発行する必要がないため、ソフトウェアの変更だけですぐにシステムを導入できる。照合計算部１３がＩＣカード３ａ上にないためＩＣカードへの負荷を小さくできる。

【００８３】なお、上記動作例ではバーチャルモールでの買い物の場合で説明したが、より具体的には、例えばＳＥＴ (Secure Electronic Transaction)の購入要求への導入が考えられる。ＳＥＴは元来磁気カードを念頭に置いた仕様であるが、実用形態としてはＩＣカード（＋パスワード）の使用もできる。カード会員による検証と購入要求における「会員の秘密鍵で署名」の処理に本実施形態で説明した技術を導入するとその有用性が高まると考えられる。

【００８４】また、本実施形態では、生体データとして指紋を用いたが、本発明はこれに限られるものでなく、掌型や声紋、網膜、顔写真等、その他種々の生体データを用いる場合にも適用することができる。また、センサ１１とＩＣカード内のデジタル署名機能部分１９，２０とが分離しているので、使用するセンサ種類の自由度を大きくすることができる。

【００８５】さらに、本実施形態のシステムでは、センサモジュール１ａの生体データ保持部１２に複数の生体データをできるようにすることで、個人用のシステムとしてだけでなく、多数人が同一システムを使用できるようにすることも可能である。

（発明の第２の実施の形態）図３は本発明の第２の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００８６】このユーザ確認システムは、図１５の候補システムのうちの万能ＩＣカード型であり、センサモジュール１ｂと、コンピュータ２ｂと、ＩＣカード３ｂとから構成されている。本システムでは、センサモジュール１ｂではセンサ入力情報送信のみ（簡単なスクランブル処理は行う）を行い、ＩＣカード３ｂ側で署名処理に加えて生体データ保持と照合計算を行う。

【００８７】図３に示す各構成におけるセンサ１１、生体データ保持部１２、照合処理部１３、確認処理部１７、演算処理部１９及び秘密鍵保持部２０の機能は第１の実施形態の図１に示されるものと同様である。ただし、その各部の配置場所が異なっている。

【００８８】すなわち、本実施形態では、センサモジュール１ｂにはセンサ１１のみが設けられている。一方、ＩＣカード１ｂには、生体データ保持部１２、照合処理部１３、確認処理部１７、演算処理部１９及び秘密鍵保持部２０が設けられ、これらは同一ＩＣチップ内に構成される。なお、コンピュータ２ｂの構成は第１実施形態のコンピュータ２ａと同様である。

【００８９】各部がこのように配置されることからセンサモジュール１ｂにはそれほど高い耐タンパー性は必要ないが、ＩＣカード３ｂには高い耐タンパー性が要求され、第１の実施形態で説明したような手段で耐タンパー性が確保されている。

【００９０】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【００９１】ここでも第１の実施形態と同様にインターネット４上のバーチャルモールへのアクセスを例にとって説明する。

【００９２】図４は本実施形態の動作例を示す流れ図である。

【００９３】同図において、ステップＳＴ１１からＳＴ１３までの処理は第１の実施形態の図２ステップＳＴ１からＳＴ３までと同様である。

【００９４】次に、センサモジュール１ｂからは測定されたセンサ情報がＩＣカード３ｂに送出される（ＳＴ１４）。センサ情報を受け取ったＩＣカード３ｂでは第１の実施形態のセンサモジュール１ａ内で処理と同様な照合が実行される（ＳＴ15）。なお、この照合処理はＩＣカード３ｂ内のみで行われるので、耐タンパー性を高めるため、生体データ保持部１２の生体データはＩＣカード３ｂから外部に出力できない構成となっている。

【００９５】照合により本人確認がなされると（ＳＴ１６）、その確認結果が演算処理部１９に通知され（ＳＴ１７）、以下第１実施形態と同様に、デジタル署名等行われ（ＳＴ１８）、演算されたメッセージＣがバーチャルモールへ出力される（ＳＴ１９）。

【００９６】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、照合処理部１３と生体データ保持部１２を同一のＩＣカード３ｂに格納するとともに、当該カード３ｂの耐タンパー性を高くしたので、生体データの漏洩危険性を低減させることができるとともに、生体データを高い安全性でもってユーザ手元の管理範囲（ＩＣカード）に置いて守ることができ、自己の生体データを情報機器を格納することに対するユーザの抵抗感を大幅に低減させることができる。つまり、個人所有するＩＣカードにセンサ以外の主要な要素がすべて実装されているため、心理的にも安心感が強い。

【００９７】また、照合計算部１３と演算処理部１９が同一ＩＣチップ内に構成されるので、本人を確認してからデジタル署名するまでの処理を安全に行うことができ、極めてセキュリティの高いＩＣカード署名システムを実現することができる。

【００９８】また、本実施形態のシステムでは、センサモジュール側では比較的原始的な信号処理のみを受け持たせているので、センサモジュール１ｂの負担を小さくすることができる。

【００９９】万能ＩＣカード型は照合装置に対して特別な要請は無く、どの型の指紋照合装置でも適用可能である。このシステムのセキュリティはもっぱらＩＣカードの耐タンパー性に基づいており、暗号通信を用いた工夫は行っていないためシンプルな構造となっている。ＩＣカード３ｂに多くの機能（生体データ保持、照合計算部、署名処理、署名鍵保持、）を持たせたため、ＩＣカード３ｂへの負荷は大きい。したがって、この用途に限定した専用のＩＣカードを発行するとより効果的なシステム運用が可能となる。

【０１００】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【０１０１】（発明の第３の実施の形態）図５は本発明の第３の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１０２】このユーザ確認システムは、図１５の候補システムのうちのＩＣカードにデータ～センサ計算型であり、センサモジュール１ｃと、コンピュータ２ｃと、ＩＣカード３ｃとから構成されている。本システムでは、センサモジュール側で照合計算を行い、ＩＣカード側に生体データを保持する。

【０１０３】センサモジュール１ｃは、スタンドアロン型であり、センサ１１と、照合計算部１３と、同定文字列保持部１４と、復号処理部２１と、復号鍵保持部２２とから構成されている。

【０１０４】また、ＩＣカード３ｃは、確認処理部１７と、同定文字列保持部１８と、演算処理部１９と、秘密鍵保持部２０と、暗号化生体データ保持部１２ｂとから構成されている。ここで、センサモジュール１ｃ及びＩＣカード３ｃは耐タンパー性の高い構成となっている。

【０１０５】ＩＣカード３ｃにおける暗号化生体データ保持部１２ｂには、ＩＣカード保持者の生体データが復号鍵保持部２２に格納される復号鍵で復号できるように暗号化され保持されている。

【０１０６】また、センサモジュール１ｃの復号処理部２１は、ＩＣカード３ｃから受け取った暗号化生体データを復号鍵保持部２２に格納される復号鍵で復号して照合計算部１３に提供するようなっている。

【０１０７】なお、コンピュータ２ｃは、第１の実施形態と同様に構成される。

【０１０８】このように構成された本発明の実施の形態に係る生体データによるユーザ確認システムは次に説明するように動作する。

【０１０９】ここでも第１の実施形態と同様にインターネット４上のバーチャルモールへのアクセスを例にとって説明する。

【０１１０】図６は本実施形態の動作例を示す流れ図である。

【０１１１】同図に示す本実施形態の生体データによるユーザ確認システムにおいて、コマンド出力（ＳＴ２１）及びＩＣカード挿入（ＳＴ２２）、並びに、センサによる生体測定が行われ（ＳＴ２５）、センサモジュールにおけるセンサ情報と生体データの照合された以降の処理（ＳＴ２６～ＳＴ３１）は、図２に示す第１の実施形態の場合（図２：ＳＴ１～ＳＴ２並びにＳＴ３～ＳＴ９）と同様である。したがって、この部分の処理は説明を省略する。

【０１１２】本実施形態の特徴は、ＩＣカード３ｃに保持された暗号化生体データがＩＣカード３ｃからセンサモジュール１ｃに送出されるとともに（ＳＴ２３）、その生体データがセンサモジュール１ｃ内の復号処理部２１及び復号鍵保持部２２の復号鍵により復号され（ＳＴ２４）、ステップＳＴ２６の照合計算に提供されるところにある。

【０１１３】本人確認並びにデジタル署名等の処理体系をこのような構成動作としたことによる効果について以下に説明する。

【０１１４】本発明の実施の形態に係る生体データによるユーザ確認システムは、個人が所有する演算（例えばデジタル署名）機能付きＩＣカード３ｃに本人の生体データを保持し、暗号化された生体データを特定の場所に常置されたセンサモジュール１ｃに送って当該センサモジュール１ｃにて照合計算を行うようにし、さらにセンサモジュール１ｃ及びＩＣカード３ｃに高い耐タンパー性を持たせたので、生体データが漏洩したりＩＣカードが他人に不正に使用されたりすることなく、安全に演算（例えばデジタル署名）を行うことができる。

【０１１５】また、生体データは暗号化されてＩＣカード３ｃのみに格納されているので、生体データの漏洩危険性を低減させることができるとともに、生体データを高い安全性でもってユーザ手元の管理範囲（ＩＣカード）に置いて守ることができ、自己の生体データを情報機器を格納することに対するユーザの抵抗感を大幅に低減させることができる。

【０１１６】さらに、本実施形態のシステムは、多くのバイオメトリクスセンサ（掌型、網膜など）はその大き

さや仕組みからＩＣカード上に実装できないことや、照合計算をＩＣカードの中で行うには比較的負荷が大きいことを考え合わせると、様々な組み合わせの中でも作り易くバランスの良いシステムとなっている。

【０１１７】しかしながら、照合を行う度に毎回ＩＣカードから個人の生体データをセンサモジュールの照合計算部１３へ送る必要があるため、セキュリティ保持のために上記した暗号化処理が行われている。図５は、なるべく簡素でありながら十分なセキュリティを保つことのできる例として、センサ側に保持された復号鍵によって暗号化された生体データをＩＣカードに保持するシステムとなっている。ＩＣカード３ｃに生体データがあり、高いセキュリティが保持される。

【０１１８】したがって、本実施形態のシステムは、不特定多数で簡単に利用可能、つまり本システムに対応した多くの場所（システム）で使用可能であり利便性が高い。すなわち、ＩＣカードに個人の生体データを持つため、一つのシステムを不特定多数で使う場合に適している。ただし、ＩＣカードに生体データを格納する必要があるため、署名用に作られたＩＣカードにさらに生体データ専用のメモリが追加されている。

【０１１９】構造的にはこのメモリと署名処理の部分は切り分けられるため、第２の実施形態で示した万能ＩＣカード型の場合に比べればＩＣカードの設計変更は容易である。また、照合計算をセンサモジュール１ｃで行うのでＩＣカード３ｃの負荷も小さく、現実的なシステムとすることができる。なお、ハッカーによる同定文字列の盗聴の危険性を排除するためには同定文字列を暗号化してＩＣカードに送るのが好ましいことは第１の実施形態と同様である。

【０１２０】また、暗号化生体データは毎回そのまま同じものをＩＣカード３ｃからセンサモジュール１ｃ側に送っているが、登録データと全く同一のセンサ情報は受け付けないという簡単な仕組みを照合計算部１３内に設けると、より高いセキュリティが保たれる。というのは通常バイオメトリクスセンサからの情報には誤差があり、登録されているデータと全く同一のデータが取得されることは殆ど有り得ないからである。全く同一のデータを拒否することにより正規ユーザの使用を妨げること無く、不正なコピーなどによって登録データ（生体データ）を入手した侵入者の使用を排除できるという効果が期待される。

【０１２１】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【０１２２】（発明の第４の実施の形態）図７は本発明の第４の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１２３】このユーザ確認システムは、図１５の候補システムのうちのＩＣカードにデータ～ＰＣ計算型であり、センサモジュール１ｄと、コンピュータ２ｄと、ＩＣカード３ｄとから構成されている。このシステムでは、センサモジュール側ではセンサ入力情報送信のみ（簡単なスクランブル処理は行う）を行い、ＩＣカード１ｄに生体データを保持し、コンピュータ（ＰＣ）で照合計算を行う。

【０１２４】本実施形態のユーザ確認システムでは、ＩＣカード３ｄ自体は、第３の実施形態のＩＣカード３ｃと同様に構成され、センサモジュール１ｄは、第２の実施形態のセンサモジュール１ｂと同様に構成されている。

【０１２５】また、コンピュータ２ｄには、第１の実施形態と同様な構成に加え、第３の実施形態のセンサモジュール１ｃにおけるセンサ１１以外の構成部分が照合機能部２３として設けられている。なお、この照合機能部２３は、照合計算部１３と、同定文字列保持部１４と、復号処理部２１と、復号鍵保持部２２とからなっており、ＤＬＬ（ダイナミック　リンク　ライブラリ）として構成させることも可能である。なお、ＤＬＬは、コマンドがスタートしたときに初めて呼ばれるプログラムである。

【０１２６】このように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【０１２７】図８は本実施形態の動作例を示す流れ図である。

【０１２８】同図に示すように、本実施形態のユーザ確認システムは、ステップＳＴ４３～ＳＴ４８の処理がセンサモジュール１ｄでなくコンピュータ２ｄにより若しくはコンピュータ２ｄに対して行われる点を除けば、図６に示す第３の実施形態のシステムと同様に動作する。

【０１２９】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、コンピュータ２ｄの内部に照合機能部２３を設けるようにしたので、ある程度の生体データの漏洩危険性の低減、並びに、確実性の高い本人確認機能，すなわちＩＣカードが紛失したり、盗まれた場合でも第３者による悪用の防止を可能としつつ、これらの機能を簡単なハードウエアで実現し経済的でかつ現実性の高いシステムとすることができる。

【０１３０】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【０１３１】（発明の第５の実施の形態）図９は本発明

の第５の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１３２】このユーザ確認システムは、図１５の候補システムのうちのＩＣカード一体型であり、コンピュータ２ｅと、ＩＣカード３ｅとから構成されている。

【０１３３】本実施形態のＩＣカード３ｅには、センサ１１、生体データ保持部１２、照合処理部１３、演算処理部１９及び秘密鍵保持部２０が設けられており、これらの各構成がセンサ１１も含めてＩＣの１チップ内に納められている。また、生体データは耐タンパー性を高めるために外部に出力できないように構成されており、ＩＣカード３ｅには、耐タンパー性を高めるための上記各仕組みが設けられている。

【０１３４】なお、コンピュータ２ｅは、アクセス対象がＩＣカード３ｅのみであることを除けば第１の実施形態と同様に構成されている。

【０１３５】このように構成された生体データによるユーザ確認システムの動作は、センサ１１自体がＩＣカード２ｅ内に設けられ、ＩＣカード２ｅにて生体測定が行われセンサ情報の機器間移動がない点を除けば、第２の実施形態と同様である。

【０１３６】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、第２の実施形態の構成を有するＩＣカードにさらにセンサ１１を設けて秘匿性の高い情報は全てＩＣカード３ｅの内部で処理するようにしたので、第２の実施形態とその構成が共通する部分について同様な効果が得られる他、暗号通信を用いた工夫は不要でありシンプルなプロトコル構造とすることができる。また、耐タンパー性自体も高いものとすることができる。

【０１３７】（発明の第６の実施の形態）本実施形態は、計算機ソフトウェアの使用権限を、生体データを利用したバイオメトリクスによる個人認証で確認するシステムである。本システムは、ＩＣカード等の耐タンパー性の携帯物を使用することなく、また、生体データが漏洩したり他人に不正に使用されたりすることなく、ソフトウエアの使用許可を安全に行うものである。

【０１３８】図１０は本発明の第６の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１３９】このユーザ確認システムは、センサモジュール１ｆとコンピュータ２ｆとから構成されている。

【０１４０】センサモジュール１ｆは、第２実施形態と同様に構成されており、センサ１１を備えたものである。

【０１４１】コンピュータ２ｆには、照合計算部３１ａと、暗号化生体データ保持部３２ａと、スクリーンセーバー等の起動対象ソフトウエア３４ａが設けられている。

【０１４２】暗号化生体データ保持部３２ａには、各ユーザのログオンパスワードで予め暗号化された各ユーザの生体データが保持されている。

【０１４３】照合計算部３１ａは、生体データとセンサ測定情報により個人認証を行い、使用権限者と確認できれば対象ソフトウェア３４ａに起動命令を出力する。

【０１４４】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【０１４５】まず、対象ソフトウェア３４ａを使い始める際に、ユーザにより入力装置（図示せず）を介してログオンパスワード３３ａが入力される。

【０１４６】次に照合計算部３１ａにより、対象ソフトウエア３４ａの使用権限を有する暗号化生体データが生体データ保持部３２ａから読み出され、入力ログオンパスワード３３ａによる復号化が行われる。

【０１４７】次に、センサモジュール１ｆにおいて生体測定が行われ、その測定結果がコンピュータ２ｆの照合計算部３１ａに送信される。なお、この送信データには簡単なスクランブルがかけられている。

【０１４８】照合計算部３１ａでは、復号化された生体データと、受信したセンサ情報を照合し、システムを使用している者が起動対象のソフトウエア３４ａの使用権限を有するか否かを確認する。なお、ログオンパスワード３３ａ、復号化された生体データ及び受信したセンサ情報は揮発性メモリ上にのみ記録され、セッション終了後はこれらの情報は消えるようになっている。

【０１４９】上記照合計算により、ソフトウエア起動の要求をしている者が正当な使用権限を有するユーザ本人であると確認されると、照合計算部３１ａによりその旨が起動対象ソフトウエア３４ａに通知される。これにより、起動対象ソフトウエアの起動処理が開始される。

【０１５０】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、ログオンパスワード３３ａを入力することにより、当該ログオンパスワードで暗号化された生体データが復号され、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、パスワードで暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。

【０１５１】さらに、パスワード等は揮発性メモリ上にのみ記録され、セッションを終了すると情報は消え去るため、何らかの手段でハードディスク等に記録された不揮発性の情報を読まれることがあってもパスワード情報等が盗まれることはない。

【０１５２】なお、本実施形態では、ソフトウエア使用権限の場合で説明したが、本発明はソフトウエア起動の

場合に限られるものでなく、例えば計算機自体の起動や各種機器の起動についても本実施形態の技術を適用させることができる。

【０１５３】また、例えば本実施形態の技術を用いてユーザ確認及び権限確認をしつつ計算機の起動をした場合に、そのユーザが使用権限を有するソフトウエアのリストを表示し、以降、リスとアップされたソフトウエアの使用は自由にできるようにしてもよい。このようにすれば、ソフトウエア起動時に一々生体測定をする必要がなく、ユーザの負担を軽減することができる。

【０１５４】（発明の第７の実施の形態）図１１は本発明の第７の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１５５】このユーザ確認システムは、センサモジュール１ｇとコンピュータ２ｇとＩＣカード３ｇとから構成されている。

【０１５６】センサモジュール１ｇは、第２実施形態と同様に構成されており、センサ１１を備えたものである。

【０１５７】コンピュータ２ｇには、照合計算部３１ｂと、起動対象ソフトウエア３４ｂとが設けられている。

【０１５８】ＩＣカード３ｇには、暗号化された生体データを保持する暗号化生体データ保持部３２ｂと、この暗号化生体データを復号するための暗号鍵を保持する暗号鍵保持部３５と、ログオンパスワードを保持するログオンパスワード保持部３６とが設けられている。なお、ＩＣカード３ｇは高い耐タンパー性を有するものである。

【０１５９】コンピュータ２ｇの照合計算部３１ｂは、生体データ及びセンサ１１の生体測定結果からユーザ本人を確認し、その結果を起動対象ソフトウエア３４ｂに通知する。

【０１６０】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【０１６１】まず、ＩＣカード３ｇが挿入されると、起動対象ソフトウエア３４ｂによりＩＣカード内のログオンパスワードが読み取られ、照合計算部３１に本人確認の依頼がなされる。

【０１６２】起動対象ソフトウエア３４ｂに依頼された照合計算部３１ｂによって、生体測定情報がセンサ１１に要求されるとともに、ＩＣカード３ｇの暗号化生体データ保持部３２ｂ及び暗号鍵保持部３５から暗号化生体データ及びその暗号鍵が読み出される。

【０１６３】これらの情報を受け取った照合計算部３１ｂは暗号化生体データを復号して生体データを取り出すとともに、センサ１１から生体測定情報を受け取り、両者を比較照合してユーザ本人か否か確認する。

【０１６４】本人であることが確認されればその旨が起動対象ソフトウエア３４ｂに通知され、起動対象ソフトウエア３４ｂの起動が開始される。

【０１６５】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、ＩＣカード３ｇをコンピュータ２ｇに挿入するだけで、暗号鍵で暗号化された生体データが復号され、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、暗号鍵で暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。

【０１６６】さらに、コンピュータにおいて生体データ等は揮発性メモリ上にのみ記録され、セッションを終了すると情報は消え去るため、これらの情報が盗まれることはない。

【０１６７】なお、本実施形態では、ソフトウエア使用権限の場合で説明したが、本発明はソフトウエア起動の場合に限られるものでなく、例えば計算機自体の起動や各種機器の起動についても本実施形態の技術を適用させることができる。

【０１６８】また、例えば本実施形態の技術を用いてユーザ確認及び権限確認をしつつ計算機の起動をした場合に、そのユーザが使用権限を有するソフトウエアのリストを表示し、以降、リスとアップされたソフトウエアの使用は自由にできるようにしてもよい。このようにすれば、ソフトウエア起動時に一々生体測定をする必要がなく、ユーザの負担を軽減することができる。

【０１６９】（発明の第８の実施の形態）本実施形態は、ファイル暗号化用の暗号鍵を記録したＩＣカードに生体データも記録することにより、暗号処理のセキュリティを高めたファイル暗号化システムとしてのユーザ確認システムを提供するものである。

【０１７０】図１２は本発明の第８の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【０１７１】このユーザ確認システムは、センサモジュール１ｈとコンピュータ２ｈとＩＣカード３ｈと二次記憶装置としてのハードディスク５とから構成されている。

【０１７２】センサモジュール１ｈは、第２実施形態と同様に構成されており、センサ１１を備えたものである。コンピュータ２ｈには、照合計算部３１ｃと、暗号化プログラム３７が設られている。また、ＩＣカード３ｈには、生体データ保持部３２ｃと、暗号計算部３８と、暗号鍵保持部３９とが設けられている。さらに、ハードディスク５には、暗号若しくは復号対象となる入力ファイル４０と、暗号若しくは復号結果としての出力ファイル４１とが設けられている。

【０１７３】照合計算部３１ｃは、生体データとセンサ

情報とからユーザ本人を確認し、暗号化プログラム３７並びに暗号計算部３８にファイル暗号化開始許可の通知をするようになっている。

【０１７４】暗号化プログラム３７は、入力ファイル４０を読み込み、その暗号若しくは復号対象情報を暗号計算部３８と協力して暗号若しくは復号し、その結果を出力ファイル４１に出力する。

【０１７５】暗号計算部３８は、暗号化プログラム３７が行う暗号若しくは復号処理の一部を担っており、自身が行うその暗号若しくは復号処理部分において暗号鍵保持部３９の暗号鍵を使用する。

【０１７６】なお、ＩＣカード３ｈは高い耐タンパー性を有するものである。

【０１７７】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【０１７８】図１３は本実施形態の全体動作を示す流れ図である。

【０１７９】まず、暗号化プログラム３７の起動を開始する（ＳＴ６１）。暗号化プログラム３７は照合計算部３１ｃにシステム使用者が本人であるか否かの確認を依頼する。

【０１８０】次に挿入されたＩＣカード３ｈから生体データが照合計算部３１ｃに読み取られる（ＳＴ６２）。なお、特に図示しないが生体データ保持部３２ｃに格納され送出される生体データは、本実施形態の方法あるいは第３の実施形態の方法等で暗号化されたものであり、照合計算部３１ｃにおいて復号化されて用いられる。

【０１８１】次に、センサ１１による生体測定が行われ、センサ情報が照合計算部３１ｃに送出される（ＳＴ６３）。なお、この送信データには簡単なスクランブルがかけられている。

【０１８２】次に、照合計算部３１ｃにて生体データとセンサ情報の照合が行われ、システム使用者がユーザ本人であるか否かの確認がなされる（ＳＴ６４）。なお、復号化された生体データ及び受信したセンサ情報は揮発性メモリ上にのみ記録され、セッション終了後はこれらの情報は消えるようになっている。

【０１８３】上記照合をした結果、本人でなければエラー表示して終了し、本人と確認されれば、その旨の通知が暗号化プログラム３７及び暗号計算部３８になされる（ＳＴ６５）。

【０１８４】これによって、暗号化プログラム３７及び暗号計算部３８の起動が終了し、ファイルの暗号化処理が開始される（ＳＴ６６）。

【０１８５】すなわち入力ファイル４０が暗号化プログラム３７に読み込まれ（ＳＴ６７）、暗号化若しくは復号化処理が実行されて（ＳＴ６８）、その結果が出力ファイルに出力され（ＳＴ６９）、一連の処理が終了する。

【０１８６】次に、ステップＳＴ６８における暗号化処理について詳しく説明する。

【０１８７】図１４は本実施形態における暗号化処理を示す流れ図である。

【０１８８】まず、暗号化プログラム３７において、暗号化の鍵として乱数が発生され（ＳＴ７１）、当該乱数を鍵として読み込まれた暗号化対象データ（平文）が暗号化される（ＳＴ７２）。

【０１８９】この乱数はＩＣカード３ｈ内の暗号計算部３８に送出され（ＳＴ７３）、この暗号計算部３８において暗号鍵保持部３９内の暗号鍵により暗号化される（ＳＴ７４）。

【０１９０】暗号化した乱数は暗号計算部３８によってコンピュータ２ｈの暗号化プログラム３７に送出される（ＳＴ７５）。

【０１９１】受信された暗号化乱数は、暗号化プログラム３７によってステップＳＴ７２で平文を暗号化した暗号文のヘッダとして付加され、全体として一つの暗号文が構成される（ＳＴ７６）。すなわち、ステップＳＴ７２で暗号化されたものを暗号文本体とし、ステップＳＴ７５で暗号化された乱数をヘッダとして暗号文を生成する。

【０１９２】こうして生成された暗号文がハードディスク５に出力されることになる。

【０１９３】一方、図１３のステップＳＴ６８における復号化処理は上記暗号化処理の逆の処理が行われることになる。

【０１９４】すなわちまず、暗号化プログラム３７は、復号対象の暗号文におけるヘッダのみを暗号計算部３８に送り、暗号計算部３８ではそのヘッダを暗号鍵保持部３９内の鍵で復号する。

【０１９５】こうして復号された情報は、復号対象の暗号文の本文を暗号化するのに用いた鍵としての乱数である。

【０１９６】この取り出された乱数が暗号計算部３８から暗号化プログラム３７に送出される。この乱数を受信した暗号化プログラム３７は、受信乱数により暗号文本文を復号し、もとの平文を取り出す。

【０１９７】こうして復号された平文がハードディスク５に出力されることになる。

【０１９８】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、生体データ及び乱数用の暗号鍵を耐タンパー性の高いＩＣカード３ｈに格納するようにしたので、極めて秘匿性の高い暗号化処理を確実にユーザ本人確認してから実行することができる。

【０１９９】また、本実施形態では乱数を用いた間接的な暗号化処理を行うようにしたので、暗号化処理と復号処理を行うたびに異なる乱数が使われ、万一１個の乱数が解読されても、次回の暗号化処理と復号処理の秘密は

守られ、確実なユーザ確認と高セキュリティと兼ね備えた暗号化システムを実現することができる。

【０２００】さらに、上記暗号復号処理に使用されるＩＣカード３ｈ内の暗号鍵はＩＣカード内の暗号計算部３８でのみ使われ、ＩＣカード３ｈの外部には出ることはなく、かつ、この暗号鍵は耐タンパー性の高いＩＣカード３ｈ内に格納されているので、暗号の秘匿性をより高めることができる。

【０２０１】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【０２０２】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。

【０２０３】

【発明の効果】以上詳記したように本発明によれば、生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感及び生体データの漏洩危険性を低減することを可能とし、さらに使用上の煩わしさが少なくユーザ確認の確実性が高い生体データによるユーザ確認システム及びＩＣカード並びに記録媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図２】同実施形態の動作例を示す流れ図。

【図３】本発明の第２の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図４】同実施形態の動作例を示す流れ図。

【図５】本発明の第３の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図６】実施形態の動作例を示す流れ図。

【図７】本発明の第４の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図８】同実施形態の動作例を示す流れ図。

【図９】本発明の第５の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図１０】本発明の第６の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図１１】本発明の第７の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図１２】本発明の第８の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図１３】同実施形態の全体動作を示す流れ図。

【図１４】同実施形態における暗号化処理を示す流れ図。

【図１５】バイオメトリクスを適用させたＩＣカード署名システムにおける構成要素及びその組み合わせ結果を示す図。

【符号の説明】

１ａ，１ｂ，１ｃ，１ｄ，１ｆ，１ｇ，１ｈ…センサモジュール

２ａ，２ｂ，２ｃ，２ｄ，２ｅ，２ｆ，２ｇ，２ｈ…コンピュータ

３ａ，３ｂ，３ｃ，３ｄ，３ｅ，３ｇ，３ｈ…ＩＣカード

４…インターネット等

５…ハードディスク

１１…センサ

１２…生体データ保持部

１３…照合処理部

１４…同定文字列格納部

１５…コマンド出力部

１６…メッセージ出力部

１７…確認処理部

１８…同定文字列格納部

１９…演算処理部

２０…秘密鍵保持部

２１…復号処理部

２２…復号鍵保持部

２３…照合機能部

３１ａ…照合計算部

３２ａ…暗号化生体データ保持部

３４…起動対象ソフトウエア

３７…暗号化プログラム

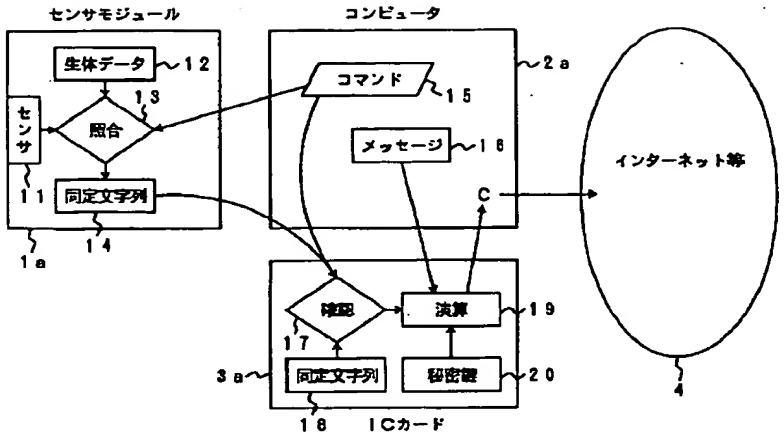
３８…暗号計算部

３９…暗号鍵保持部

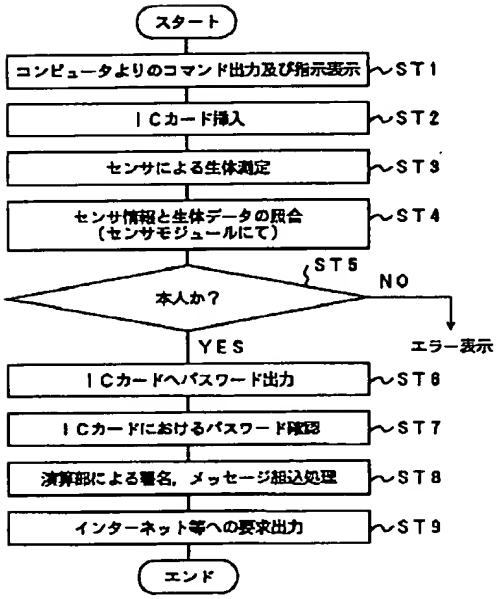
４０…入力ファイル

４１…出力ファイル

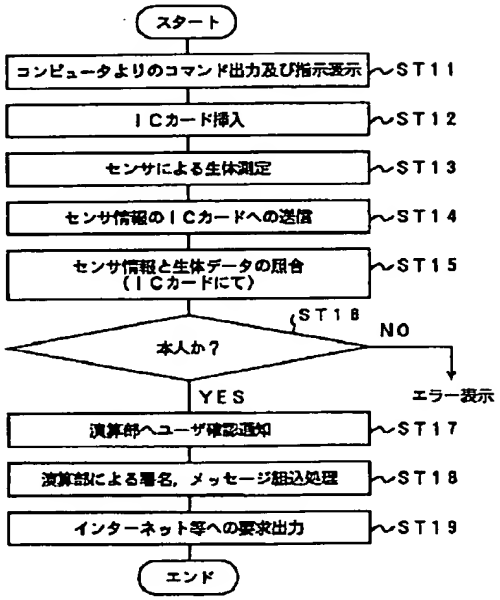
【図１】


センサモジュール
コンピュータ
生体データ
１２
１３
照合
センサ
１１
同定文字列
１４
１ａ
コマンド
１５
２ａ
メッセージ
１６
C
インターネット等
４
確認
１７
演算
１９
３ａ
同定文字列
１８
秘密鍵
２０
ＩＣカード

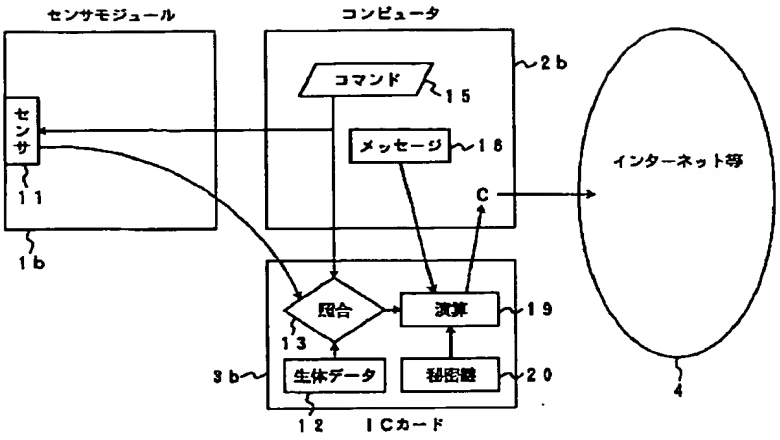
【図２】


スタート
コンピュータよりのコマンド出力及び指示表示
ST１
ＩＣカード挿入
ST２
センサによる生体測定
ST３
センサ情報と生体データの照合
（センサモジュールにて）
ST４
ST５
本人か？
NO
エラー表示
YES
ＩＣカードへパスワード出力
ST６
ＩＣカードにおけるパスワード確認
ST７
演算部による署名，メッセージ組込処理
ST８
インターネット等への要求出力
ST９
エンド

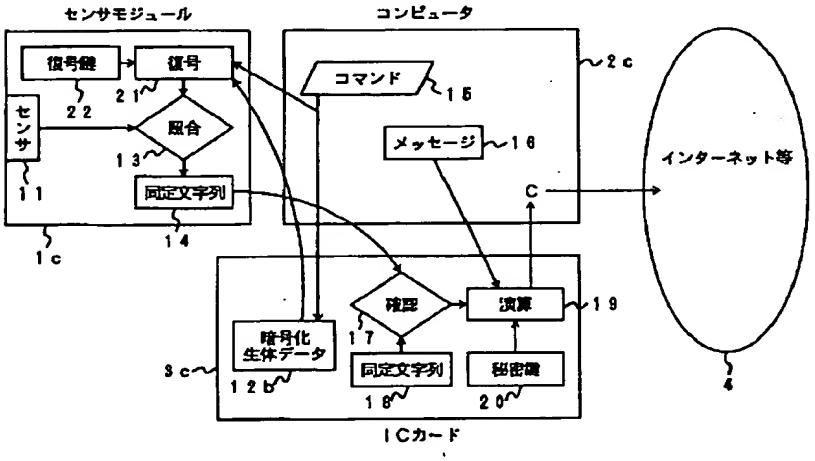
【図４】


スタート
コンピュータよりのコマンド出力及び指示表示
ST１１
ＩＣカード挿入
ST１２
センサによる生体測定
ST１３
センサ情報のＩＣカードへの送信
ST１４
センサ情報と生体データの照合
（ＩＣカードにて）
ST１５
ST１６
本人か？
NO
エラー表示
YES
演算部へユーザ確認通知
ST１７
演算部による署名，メッセージ組込処理
ST１８
インターネット等への要求出力
ST１９
エンド

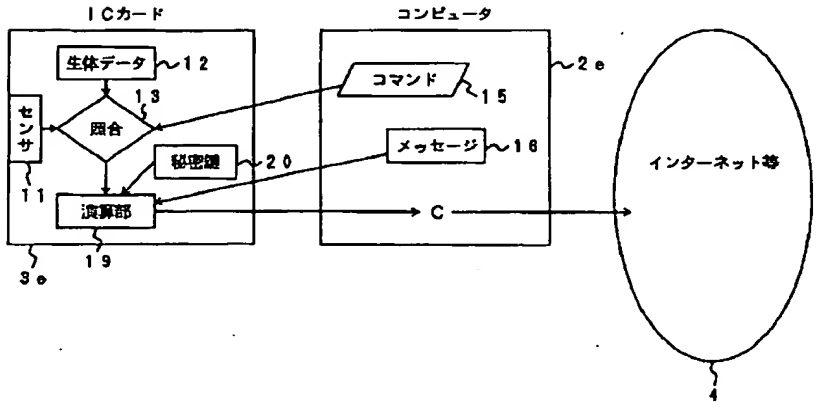
【図３】


センサモジュール
コンピュータ
2b
コマンド
15
センサ
11
メッセージ
16
インターネット等
C
1b
照合
演算
19
13
3b
生体データ
秘密鍵
20
12
ICカード
4

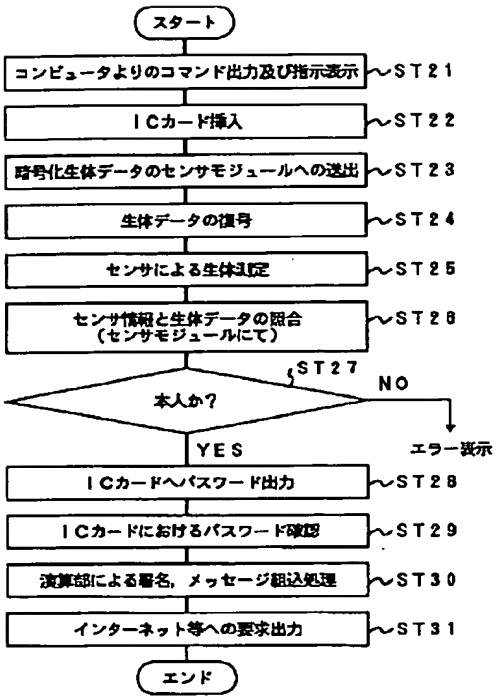
【図５】


センサモジュール
コンピュータ
復号鍵
復号
2c
コマンド
15
21
22
センサ
照合
メッセージ
16
インターネット等
13
11
同定文字列
C
1c
14
確認
演算
19
暗号化
生体データ
17
3c
同定文字列
秘密鍵
12b
16
20
ICカード
4

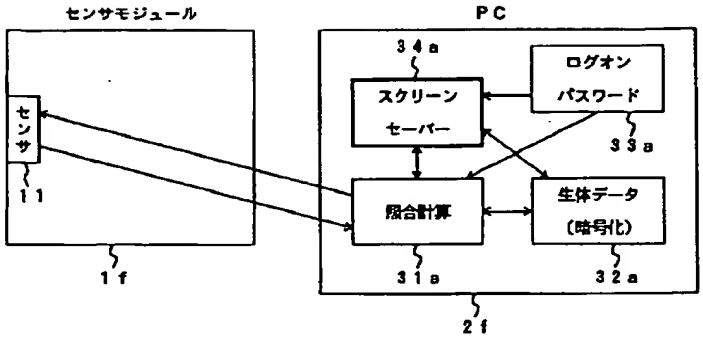
【図９】


ICカード
コンピュータ
生体データ
12
2e
コマンド
15
13
センサ
照合
メッセージ
16
インターネット等
秘密鍵
20
11
演算部
C
19
3e
4

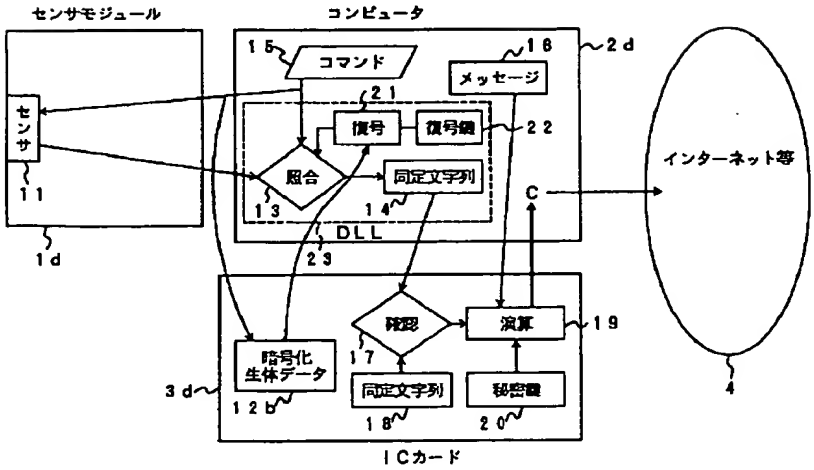
【図６】


スタート
コンピュータよりのコマンド出力及び指示表示
ST21
ICカード挿入
ST22
暗号化生体データのセンサモジュールへの送出
ST23
生体データの復号
ST24
センサによる生体測定
ST25
センサ情報と生体データの照合
（センサモジュールにて）
ST26
ST27
本人か？
NO
エラー表示
YES
ICカードへパスワード出力
ST28
ICカードにおけるパスワード確認
ST29
演算部による署名，メッセージ組込処理
ST30
インターネット等への要求出力
ST31
エンド

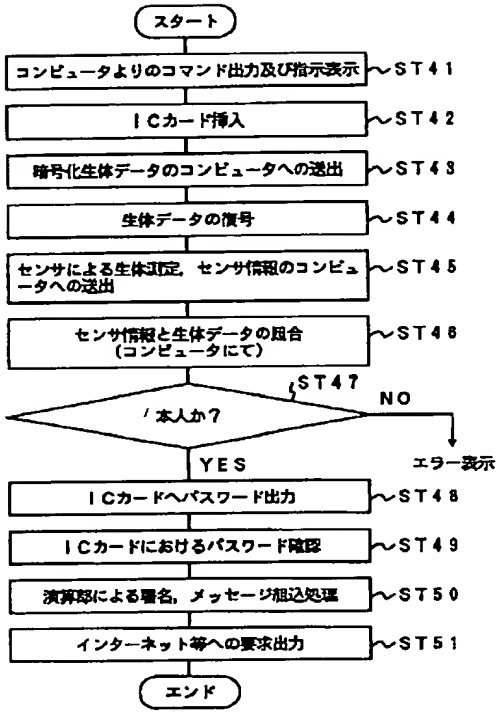
【図１０】


センサモジュール
PC
センサ
11
1f
34a
ログオン
パスワード
スクリーン
セーバー
33a
照合計算
生体データ
（暗号化）
31a
32a
2f

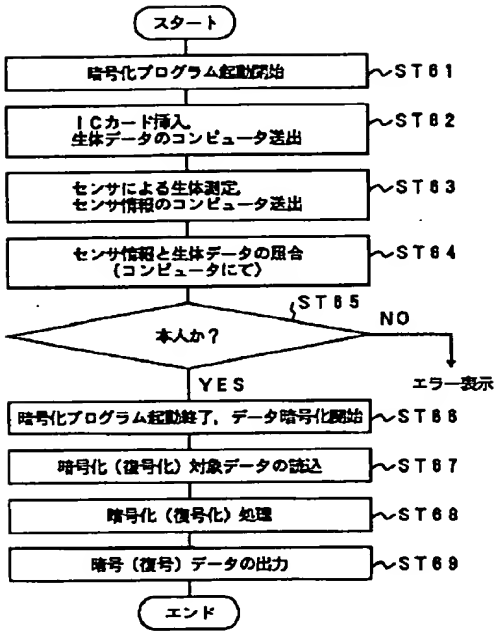
【図７】


センサモジュール
コンピュータ
センサ
11
1d
15
コマンド
16
メッセージ
2d
21
復号
復号鍵
22
照合
同定文字列
13
14
DLL
23
C
インターネット等
4
暗号化
生体データ
3d
12b
照合
17
演算
19
同定文字列
18
秘密鍵
20
ICカード

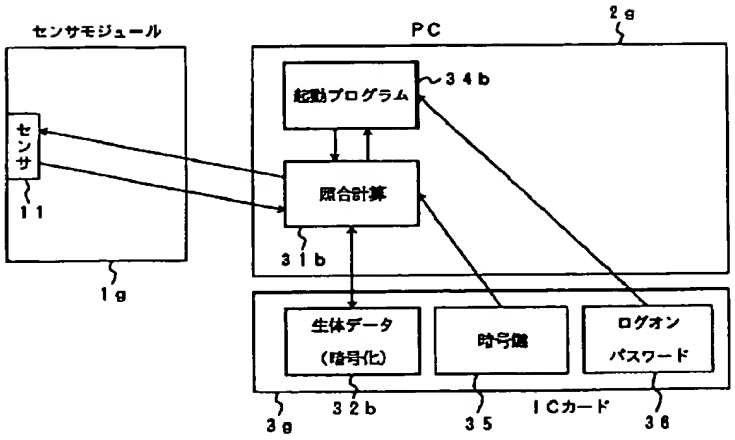
【図８】


スタート
コンピュータよりのコマンド出力及び指示表示
ＳＴ４１
ＩＣカード挿入
ＳＴ４２
暗号化生体データのコンピュータへの送出
ＳＴ４３
生体データの復号
ＳＴ４４
センサによる生体測定，センサ情報のコンピュータへの送出
ＳＴ４５
センサ情報と生体データの照合（コンピュータにて）
ＳＴ４６
ＳＴ４７
本人か？
ＮＯ
ＹＥＳ
エラー表示
ＩＣカードへパスワード出力
ＳＴ４８
ＩＣカードにおけるパスワード確認
ＳＴ４９
演算部による署名，メッセージ組込処理
ＳＴ５０
インターネット等への要求出力
ＳＴ５１
エンド

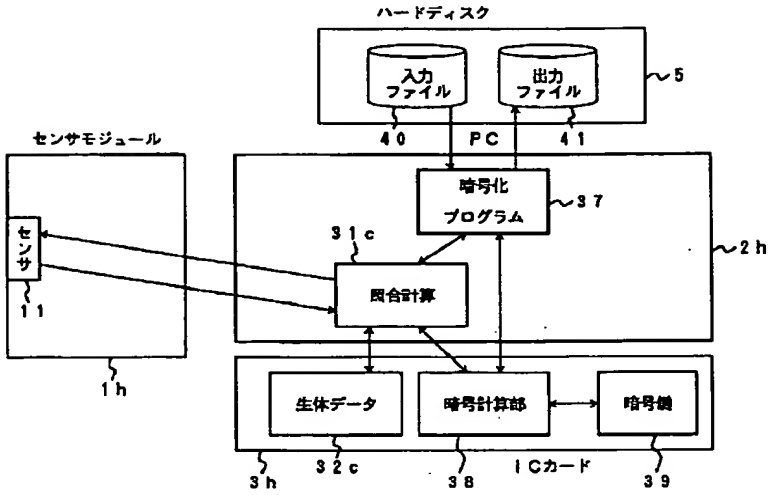
【図１３】


スタート
暗号化プログラム起動開始
ＳＴ６１
ＩＣカード挿入，生体データのコンピュータ送出
ＳＴ６２
センサによる生体測定，センサ情報のコンピュータ送出
ＳＴ６３
センサ情報と生体データの照合（コンピュータにて）
ＳＴ６４
ＳＴ６５
本人か？
ＮＯ
ＹＥＳ
エラー表示
暗号化プログラム起動終了，データ暗号化開始
ＳＴ６６
暗号化（復号化）対象データの読込
ＳＴ６７
暗号化（復号化）処理
ＳＴ６８
暗号（復号）データの出力
ＳＴ６９
エンド

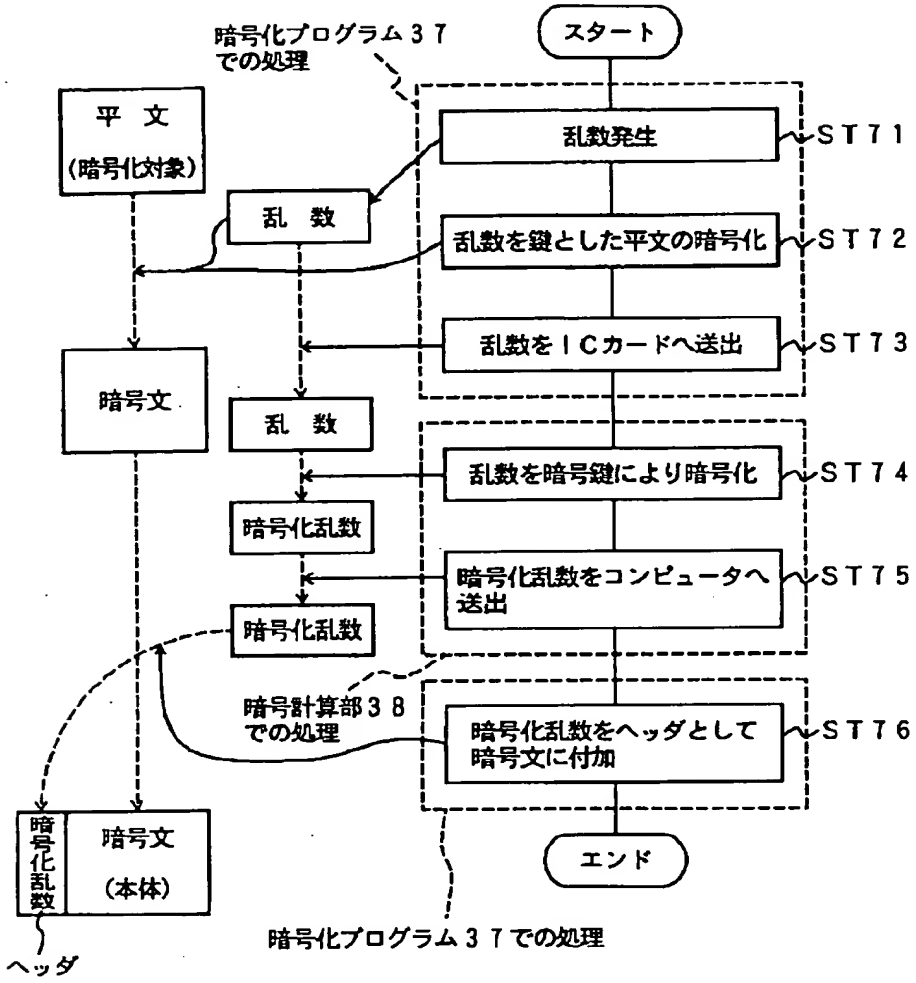
【図１１】


センサモジュール
ＰＣ
２ｇ
起動プログラム
３４ｂ
センサ
１１
照合計算
３１ｂ
１ｇ
生体データ（暗号化）
暗号鍵
ログオンパスワード
３２ｂ
ＩＣカード
３５
３６
３ｇ

【図１２】


ハードディスク
入力ファイル
出力ファイル
5
40
PC
41
センサモジュール
暗号化プログラム
37
31c
センサ
11
2h
照合計算
1h
生体データ
暗号計算部
暗号鍵
3h
32c
38
ICカード
39

【図１４】


暗号化プログラム３７
での処理
スタート
平　文
(暗号化対象)
乱数発生
ＳＴ７１
乱　数
乱数を鍵とした平文の暗号化
ＳＴ７２
乱数をＩＣカードへ送出
ＳＴ７３
暗号文
乱　数
乱数を暗号鍵により暗号化
ＳＴ７４
暗号化乱数
暗号化乱数をコンピュータへ
送出
ＳＴ７５
暗号化乱数
暗号計算部３８
での処理
暗号化乱数をヘッダとして
暗号文に付加
ＳＴ７６
暗号化乱数
暗号文
(本体)
エンド
ヘッダ
暗号化プログラム３７での処理

[図15]

	候補システム	ICカード	センサ	PC&R/W	サーバー	照合装置のタイプ	備　考
第5実施形態	ICカード一体型	生体，照合				1チップ	理想的
第1実施形態	耐タンパーモジュール一体型	PIN	PIN，生体，照合			1チップ，スタンドアロン	従来カード利用可
第2実施形態	万能ICカード型	生体，照合				従来型	準理想的
第3実施形態	ICカードにデーターセンサ計算型	生体	照合			スタンドアロン	一般的，カードに機能付加要
第4実施形態	ICカードにデーターPC計算型	生体，文字列		文字列，照合		従来型	一般的，カードに機能付加要，依頼計算の検討要
	（参考例1）	生体			照合	従来型	一般的，カードに機能付加要
	（参考例2）		生体	照合		メモリ内蔵型	変形例，従来カード利用可
	（参考例3）		生体		照合	メモリ内蔵型	変形例，従来カード利用可
	（参考例4）	照合	生体			メモリ内蔵型	変形例
	（参考例5）				生体，照合	従来型	従来カード利用可
	（参考例6）			生体（暗号化），照合		従来型	従来カード利用可

生体データと照合計算の配置可能性